METHOD AND SYSTEM FOR IMAGE VERIFICATION TO PREVENT MESSAGING ABUSE

Cross Reference To Related Application

This Utility Application claims priority from U.S. Provisional Application No. 60/460,707, filed April 4, 2003, the benefit of the earlier filing date is hereby claimed under 35 U.S.C. 119(e).

Field Of The Invention

The present invention is generally directed to electronic mail (email), and more particularly, to employing a challenge to verify outbound email traffic associated with an email account.

Background of the Invention

Recently, tools for administrators of email systems have become available to prevent their clients from receiving unsolicited/unauthorized inbound email (spam). For example, several types of firewalls and customizable filters are available to prevent inbound spam email. Adaptive filters, such as those based on bayesian probability models, have also been relatively effective in preventing some of the more sophisticated spam email, such as spam that tries to obfuscate source addresses and/or general content. Although tools to manage inbound spam email have improved in efficiency and efficacy, the "spammers" have become equally ingenious in devising ways to beat the latest preventive methods. Also, the amount of system resources that must be dedicated to handling the seemingly ever increasing amount of inbound spam email can seriously reduce the amount of resources available for legitimate email traffic.

Although email administrators have had access to a wide variety of methods to prevent inbound spam emails for some time, preventing the abuse of an email system employed to originate outbound spam email has not received the same degree of attention. Notably, most spam prevention methods are directed to stopping inbound spam email, not outbound. Also, it has become known that a significant portion of spam email originates in email systems that enable anyone to anonymously sign up for multiple email accounts. Unfortunately, spammers are known to abuse this anonymity by automating the

sending of large amounts of spam email from multiple email accounts, often to users of the same email system. To prevent such abuse, email administrators could benefit from a method that could challenge a particular client's outbound email usage that exceeds certain limits in a manner that is incompatible with an automated response, i.e., a challenge that is easily solved by a human being and difficult to answer for an automated computer program such as those employed by spammers.

Brief Description of the Drawings

Non-limiting and non-exhaustive embodiments of the present invention are described with reference to the following drawings. In the drawings, like reference numerals refer to like parts throughout the various figures unless otherwise specified.

For a better understanding of the present invention, reference will be made to the following Detailed Description of the Invention, which is to be read in association with the accompanying drawings, wherein:

FIGURES 1-4 show schematic diagrams of an illustrative operating environment for the present invention;

FIGUREs 5A and 5B illustrates a flow diagram for challenging a client's message usage based on an image verification test;

FIGURE 6 shows an exemplary statement that can be used in determining if a limit for the number of recipients for a particular client's message has been exceeded;

FIGURE 7 illustrates a block diagram of an exemplary image verification test based on a Gimpy Captcha challenge; and

FIGURE 8 shows a block diagram of an exemplary image verification test based on a Bongo Captcha challenge, in accordance with the present invention.

Detailed Description of the Preferred Embodiment

The present invention is now described. While it is disclosed in its preferred form, the specific embodiments of the invention as disclosed herein and illustrated in the drawings are

not to be considered in a limiting sense. Rather, these embodiments are provided so that this disclosure will be thorough and complete, and will fully convey the scope of the invention to those skilled in the art. Indeed, it should be readily apparent in view of the present description that the invention may be modified in numerous ways. Among other things, the present invention may be embodied as devices, methods, software, and so on. Accordingly, the present invention may take the form of an entirely hardware embodiment, an entirely software embodiment or an embodiment combining software and hardware aspects. The following detailed description is, therefore, not to be taken in a limiting sense.

Throughout the specification, the meaning of "a," "an," and "the" may also include plural references. The meaning of "in" includes "in" and "on." The term "coupled" means a direct connection between the items that are connected, or an indirect connection through one or more intermediary devices or components.

Briefly stated, the present invention is directed to a system and method for determining if a "spam" message is originating from a particular account by challenging a particular client's outbound message usage with a test that requires verification of content that is easily understood by a human being, but not an automated computer program such as those used by "spammers." If a limit on the number of recipient for outbound messages is exceeded, a test is presented the next time a client attempts to send a message. Also, if the client fails to successfully answer the test within a relatively short period of time, their ability to send a message is disabled. The time limit helps to prevent the batching of tests for several accounts that are used to automatically send relatively large numbers of outbound messages. Once disabled, the client can reinstate the ability to send a message by contacting a representative of the message system out of band, e.g., a telephone call to confirm legitimate outbound message use. Additionally, if the test is correctly answered or a client reinstates their account out of band, the recipient counts and the various limits are reset.

Different limits based on a recipient count of outbound messages can be calculated hourly, daily, and over the lifetime of a particular account. Also, a random number can be used for determining various recipient count limits so that the limits will vary within a range at each reset. Moreover, the type of message can include, but is not limited to, email, blog, message board, Short Message Service (SMS), Multi-Media

Message Service (MMS), instant messaging (IM), and the like.

Additionally, a profile can be generated for each client to determine different recipient count limits. For example, a relatively new client might have relatively low hourly, daily and lifetime limits for outbound messages. In contrast, the profile for a longtime client could enable the invention to provide relatively high hourly, daily, and/or lifetime limits. However, if a longtime client failed the image verification test, the profile could be modified so that the limits are reduced to those typically associated with a new client. Moreover, a client could modify their profile by paying a fee to extend their limits and/or advising in advance of certain occasions, such as holidays, birthdays, weddings, and the like.

The image test can be any type that has been shown to be difficult for a computer program to verify, but relatively simple for a human being. For example, an image based Captcha test can be employed, such as Gimpy, Bongo, Pix, and the like. In one embodiment, the number of false positives for the image test can be reduced if the content of an outbound message is further analyzed by a filtering system that identifies spam messages.

An exemplary Gimpy image test picks at least one word from a dictionary and employs various filters and effects to distort and/or deform displayed text. Next, a user is prompted to enter the displayed text in a box. For the Gimpy image test, distortions and deformations are chosen that are relatively simple for a human being to recognize the underlying text, but exceedingly difficult for a computer program to do so. An exemplary Gimpy image test is illustrated in FIGURE 7.

In a Bongo image test, a user is prompted to solve a visual pattern recognition problem. FIGURE 8 illustrates an exemplary Bongo image test where the symbols on the right are drawn with a light line weight and the symbols on the left are drawn with a heavy line weight. To solve the Bongo test, the user has to notice the predominant similarities in each group and to which group (left or right) a separate symbol belongs.

Although not shown, in a Pix image test, several different images that mostly include the same subject are distorted and then displayed. A user is prompted to enter the name of the subject to pass the Pix image test.

In another embodiment, a sound based Captcha test may be used such as Eco, instead of an image test in substantially the same manner. A visually impaired client can

make use of the Eco sound test in substantially the same manner as the image based tests discussed elsewhere in the specification. For example, to perform a sound test, a word or sequence of numbers is picked and, at random, the word or number is rendered into a distorted sound clip. Upon playing the sound clip, the user is prompted to enter the contents of the distorted sound clip. In this case, the distortion in the sound clip is chosen so that it is relatively easy for a human being to identify the content but difficult for a computer program.

Illustrative Operating Environment

FIGURES 1-4 show components of an exemplary environment in which the invention may be practiced. Not all the components may be required to practice the invention, and variations in the arrangement and type of the components may be made without departing from the spirit or scope of the invention.

FIGURE 1 shows a plurality of local area networks ("LANs") 120_{a-d} and wide area network ("WAN") 130 interconnected by routers 110. Routers 110 are intermediary devices on a communications network that expedite message delivery. On a single network linking many computers through a mesh of possible connections, a router receives transmitted messages and forwards them to their correct destinations over available routes. On an interconnected set of LANs--including those based on differing architectures and protocols--, a router acts as a link between LANs, enabling messages to be sent from one to another. Communication links within LANs typically include twisted pair, fiber optics, or coaxial cable, while communication links between networks may utilize analog telephone lines, full or fractional dedicated digital lines including T1, T2, T3, and T4, Integrated Services Digital Networks (ISDNs), Digital Subscriber Lines (DSLs), wireless links, or other communications links known to those skilled in the art. Furthermore, computers, such as remote computer 140, and other related electronic devices can be remotely connected to either LANs 120_{a-d} or WAN 130 via a modem and temporary telephone link. The number of WANs, LANs, and routers in FIGURE 1 may be increased or decreased arbitrarily without departing from the spirit or scope of this invention.

As such, it will be appreciated that the Internet itself may be formed from a vast number of such interconnected networks, computers, and routers. Generally, the term

"Internet" refers to the worldwide collection of networks, gateways, routers, and computers that use Transmission Control Protocol/Internet Protocol ("TCP/IP") and other packet based protocols to communicate with one another. An embodiment of the invention may be practiced over the Internet without departing from the spirit or scope of the invention.

The media used to transmit information in communication links as described above illustrates one type of computer-readable media, namely communication media. Generally, computer-readable media includes any media that can be accessed by a computing device. Computer-readable media may include computer storage media, communication media, or any combination thereof.

Communication media typically embodies computer-readable instructions, data structures, program modules, or other data in a modulated data signal such as a carrier wave or other transport mechanism and includes any information delivery media. The term "modulated data signal" means a signal that has one or more of its characteristics set or changed in such a manner as to encode information in the signal. By way of example, communication media includes wired media such as twisted pair, coaxial cable, fiber optics, wave guides, and other wired media and wireless media such as acoustic, RF, infrared, and other wireless media.

FIGURE 2 shows an exemplary server that may operate to provide a World Wide Web site (web site), and a message system, among other things. When providing a web site, server 200 transmits pages to a browser application executing on the requesting devices to carry out this process. For instance, server 200 may communicate pages and forms for setting up a messaging account for the user. Moreover, server 200 may transmit pages to a requesting device that allow the user to participate in a web site, such as send email to another user. The transactions may take place over the Internet, WAN/LAN 100, or some other communications network known to those skilled in the art.

Those of ordinary skill in the art will appreciate that the server 200 may include many more components than those shown in FIGURE 2. However, the components shown are sufficient to disclose an illustrative environment for practicing the present invention. As shown in FIGURE 2, server 200 is connected to WAN/LAN 100, or other communications network, via network interface unit 210. Those of ordinary skill in the

art will appreciate that network interface unit 210 includes the necessary circuitry for connecting server 200 to WAN/LAN 100, and is constructed for use with various communication protocols including the TCP/IP protocol. Typically, network interface unit 210 is a card contained within server 200.

Server 200 also includes processing unit 212, video display adapter 214, and a mass memory, all connected via bus 222. The mass memory generally includes random access memory ("RAM") 216, read-only memory ("ROM") 232, and one or more permanent mass storage devices, such as hard disk drive 228, a tape drive (not shown), optical drive 226, such as a CD-ROM/DVD-ROM drive, and/or a floppy disk drive (not shown). The mass memory stores operating system 220 for controlling the operation of server 200. Basic input/output system ("BIOS") 218 is also provided for controlling the low-level operation of server 200.

The mass memory as described above illustrates another type of computer-readable media, namely computer storage media. Computer storage media may include volatile and nonvolatile, removable and non-removable media implemented in any method or technology for storage of information, such as computer readable instructions, data structures, program modules or other data. Examples of computer storage media include RAM, ROM, EEPROM, flash memory or other memory technology, CD-ROM, digital versatile disks (DVD) or other optical storage, magnetic cassettes, magnetic tape, magnetic disk storage or other magnetic storage devices, or any other medium which can be used to store the desired information and which can be accessed by a computing device.

The mass memory may also store program code and data for providing a web site. More specifically, the mass memory may store applications including WWW server application 230, message server application 231, and programs 234. WWW server application 230 includes computer executable instructions which, when executed by server 200, generate browser displays, including performing the logic described above. Server 200 may include a JAVA virtual machine, an SMTP handler application for transmitting and receiving messages, an HTTP handler application for receiving and handing HTTP requests, and an HTTPS handler application for handling secure connections. The HTTPS handler application may also be used for communication with an external security application to send and receive sensitive

information, such as email, in a secure fashion.

Server 200 also comprises input/output interface 224 for communicating with external devices, such as a mouse, keyboard, scanner, or other input devices not shown in FIGURE 2. Likewise, server 200 may further comprise additional mass storage facilities such as optical drive 226 and hard disk drive 228. Hard disk drive 228 is utilized by server 200 to store, among other things, application programs, databases, and program data used by message server 231 and WWW server 230.

FIGURE 3 depicts several components of client computer 300. Those of ordinary skill in the art will appreciate that client computer 300 may include many more components than those shown in FIGURE 3. However, it is not necessary that those generally-conventional components be shown in order to disclose an illustrative embodiment for practicing the present invention. As shown in FIGURE 3, client computer 300 includes network interface unit 302 for connecting to a LAN or WAN, or for connecting remotely to a LAN or WAN. Those of ordinary skill in the art will appreciate that network interface unit 302 includes the necessary circuitry for such a connection, and is also constructed for use with various communication protocols including the TCP/IP protocol, the particular network configuration of the LAN or WAN it is connecting to, and a particular type of coupling medium. Network interface unit 302 may also be capable of connecting to the Internet through a point to point protocol ("PPP") connection or a serial line internet protocol ("SLIP") connection as known to those skilled in the art.

Client computer 300 also includes BIOS 326, processing unit 306, video display adapter 308, and memory. The memory generally includes RAM 310, ROM 304 and a permanent mass storage device, such as a disk drive. The memory stores operating system 312 and programs 334 for controlling the operation of client computer 300. The memory also includes message client 315 for accessing messages over a network, and browser application 314 for accessing web sites. It will be appreciated that these components may be stored on a computer-readable medium and loaded into memory of client computer 300 using a drive mechanism associated with the computer-readable medium, such as a floppy disk drive (not shown), optical drive 316, such as a CD-ROM/DVD-ROM drive, and/or hard disk drive 318. Input/output interface 320 may also be provided for receiving input from a mouse, keyboard, or

other input device. The memory, network interface unit 302, video display adapter 308, and input/output interface 320 are all connected to processing unit 306 via bus 322. Other peripherals may also be connected to processing unit 306 in a similar manner.

FIGURE 4 illustrates an overview of an exemplary environment in which the invention operates in which multiple clients 300 can be in communication with at least one server 200 that provides message services over network 100. Although FIGURE 4 refers to client computer 300 as an exemplary client device, other types of client devices may be employed with the invention. For example, multiprocessor systems, microprocessor-based or programmable consumer electronics, network PCs, PDAs, wearable computers, and the like. These client devices may also include devices that typically connect to network 100 using a wireless communications medium, e.g., mobile telephones, smart phones, pagers, walkie talkies, radio frequency (RF) devices, infrared (IR) devices, integrated devices combining one or more of the preceding devices, and the like.

Illustrative Image Verification Method

FIGUREs 5A and 5B illustrate a flow chart for exemplary actions for employing an image based test to verify outbound message activity is initiated by a human being instead of a computer program that automatically sends "spam" messages to other messaging accounts. Outbound message activity that exceeds at least one limit causes message functionality to be disabled until a human being can verify the message usage.

In FIGURE 5A, the process moves from a start block to block 502 where in response to a request from a client, a page that enables a client to compose a message is displayed. At block 504, the process detects if the send message command has been selected for a message composed in the page. After the send command is detected, the process steps to decision block 506 where recipient count is compared to at least one of a client's limits, e.g., hourly, daily, and lifetime. Exemplary methods for determining these limits are shown in FIGURE 6 and discussed in greater detail below. Also, if the process determines at decision block 506 that none of the limits are exceeded, then it moves to decision block 507. At decision block 507, a determination is made whether there is an indication that the message is spam. This indication may be provided by one or more filters that detect

message content and/or a recipient(s) that has an association with spam. If the determination at decision block 507 is false (no spam indicated), then the process advances to block 520 where the message system sends the composed message to each of the intended recipients. Next, the process advances to a return block and returns to performing other actions.

Alternatively, at decision block 506, if the process does determine that a recipient limit has been exceeded, it flows to block 508 (FIGURE 5B) where a verify image page is displayed. Also, at if the determination at decision block 507 was affirmative (spam indicated), the process would move to block 508 and perform substantially the same actions. In one embodiment, a Captcha image test may be employed, such as Gimpy, Bongo, Pix, and the like. In another embodiment (not shown), a sound based test, such as an Eco sound test, can be employed in substantially the same manner, either in combination with the image test or separate.

In FIGURE 5B, the process flows from block 508 to block 510 where the process waits for an attempt to verify the image test. If the attempt has occurred or a determined period of time has been exceeded, the process moves to decision block 512. The process determines if the predetermined period of time to solve the image test has expired. If affirmative, the process moves to block 522 where at least the ability to send a message is disabled for the client. The process moves to block 524 where a verification error page is displayed, which typically displays information that the client can use to contact a representative of the message system to reinstate the disabled messaging functionality. Next, the process flows to a return block and returns to performing other actions.

However, at decision block 512, if the process determines that the time period to solve the test has not expired, it moves to decision block 514. Here, another determination is made whether the total number of attempts to solve the test has been exceeded. If affirmative, the process jumps to block 522 and performs substantially the same steps discussed above.

In the alternative, at decision block 514, if the process determines that the number of attempts to solve the test is not yet exceeded, it steps to decision block 516. At decision block 516, a determination is made as to whether the image test is verified, e.g., solved. If not, the process jumps back to block 508 where substantially the same actions

discussed above are performed again. However, at block 508, a different image test than the previous one is typically displayed for solving by the client.

At decision block 516, if the determination is made that the image test is verified, the process moves to block 518 where the recipient count for the client are cleared and reset. The process moves to block 520 (FIGURE 5A) and sends the message to the intended recipients. Next, the process flows to a return block and returns to performing other actions.

FIGURE 6 illustrates three different algorithms that in concert form an exemplary recipient count statement for determining if hourly, daily, or lifetime limits for a client have been met and/or exceeded. It is important to note that the introduction of a random number into the hourly and daily algorithms causes the actual recipient count limits to vary each time they are reset between some percentage of their maximum limits. The random number is typically provided between zero and one inclusive. Also, the constant number "Y" enables the image test to be displayed at some percentage that is less than the maximum limit. The recipient count statement shown is exemplary and any number of various methods could be further employed to determine limits based on other factors, such as holidays, birthdays, special events, and client profiles.

The above specification, examples and data provide a complete description of the manufacture and use of the composition of the invention. Since many embodiments of the invention can be made without departing from the spirit and scope of the invention, the invention resides in the claims hereinafter appended.